REMARKS AND ARGUMENTS

1. Summary of the Office Action

In the Office action mailed February 10, 2004:

- The Examiner rejected claim 4 under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which the Applicants regard as the invention.

- The Examiner rejected claims 1-3, 5-15, 18-19, 21, 23-25, and 27 under 35 U.S.C. §102(b) as being anticipated by "IPv6: The New Internet Protocol", Christian Huitema, (hereinafter "Huitema").

- The Examiner rejected claims 4 and 22 under 35 U.S.C. §103(a) as being unpatentable over "IPv6: The New Internet Protocol", Christian Huitema in view of "The Internet Key Exchange (IKE)" by Harkins et al., (hereinafter "Harkins").

- The Examiner rejected claims 9, 16, 20, and 26 under 35 U.S.C. §103(a) as being unpatentable over "IPv6: The New Internet Protocol", Christian Huitema in view of "RSIP Support for End-to-end IPSEC" by Montenegro et al., (hereinafter "Montenegro").

- The Examiner did not make any statements regarding claim 17, but did reject claims 18-22, which are dependent on claim 17.

2. Amendments and Pending Claims

Applicants have amended claim 4, in response to the Examiner's rejection under 35 U.S.C. §112, second paragraph, to clarify that claim 4 depends on claim 3. Now pending in this application are claims 1-27 of which claims 1, 10, 17, and 23 are independent and the remainder are dependent.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

3. Response to §102 Rejections

As noted above, the Examiner rejected claims 1-3, 5-15, 18-19, 21, 23-25, and 27 under 35 U.S.C. §102(b) as being anticipated by Huitema. The Applicants respectfully traverse the anticipation rejection of pending claims 1-3, 5-15, 18-19, 21, 23-25, and 27 because Huitema does not disclose or suggest each and every element as recited in any of these claims.

a. The Huitema Reference

Huitema discloses a method for two entities (an initiator and a responder) on a network to engage in encrypted communication after forming a security association between the two network entities. Forming the security association includes performing a key distribution sequence between the two network entities. The leading key distribution method disclosed is called Photuris and is based on a Diffie-Hellman key exchange proposal. In Photuris, the Diffie-Hellman algorithm is *preceded* by a cookie exchange. (Huitema, page 105, para. 3, lines 10-12). Following the cookie exchange, the two network entities exchange half-keys so that session keys can be computed and authenticated. (Huitema, page 110, para. 2, lines 2-3).

b. The Claimed Invention

The present invention recognizes that in certain situations, a network entity might want to employ the algorithm disclosed by the prior art (as described above) and may need or desire to generate a *unique* cookie for use in forming a security association with another network entity. In such a situation, the cookie may need to be unique to both the network entity desiring to use it, as well as to other network devices sharing network resources with the network entity.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

In the present invention, the Applicants' independent claims are directed to methods for use by a network entity to obtain unique random numbers to use as digital cookies. In particular, the claims recite methods by which two network entities coordinate the generation of a single digital cookie that may then be used by one of the two entities to e.g., initiate a prior art key exchange. The single cookie is a composite comprising a first portion and a second portion. A first network entity generates the first portion and a second network entity, having more complete knowledge of cookies in use, generates the second portion. This type of distributed cookie *generation* is not disclosed in Huitema, although the digital cookie generated may then be used as either the initiator or responder cookies described by Huitema.

With respect to claims 1, 10, 17, and 23, Huitema does not disclose or suggest a method for generating a complete x-bit digital cookie not in use on a computer network. In particular, Huitema does not disclose or suggest a method of generating a first portion of the x-bit digital cookie on a first network device, generating a second portion of the x-bit digital cookie on a second network device, and generating a complete x-bit digital cookie from the first and second portions, as claimed in claims 1 and 10. Furthermore, in particular, Huitema does not disclose or suggest using an (x-n) bit random number, an x-bit random number, and an x-bit bit mask to generate a complete digital cookie as claimed in claim 17 or using an n-bit random number and an (x-n) bit random number to create a complete x-bit digital cookie as claimed in claim 23.

Although the Examiner asserted that Huitema discloses generating a complete x-bit digital cookie not in use on a computer network, the section in Huitema cited to by the Examiner states "A different key will be used in each direction." (Huitema, page 111, 1st

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

para., line 2). Although the prior art may allow for using a different key in each direction (perhaps during a key exchange), Applicants do not find that this particular section or any other part of Huitema discloses or suggests a method of distributed generation of digital cookies not in use in a computer network.

Because Huitema does not teach or suggest each and every element of independent claims 1, 10, 17, and 23, Huitema fails to anticipate claims 1, 10, 17, and 23 under 35 U.S.C. §102(b). Further, because each of claims 2-9, 11-16, 18-22, and 24-27 depend from either claim 1, 10, 17, or 23, Huitema necessarily fails to anticipate claims 2-9, 11-16, 18-22, and 24-27 as well.

4. Response to §103 Rejections

a. Claims 4 and 22

As noted above, the Examiner rejected claims 4 and 22 under 35 U.S.C. §103(a) as being unpatentable over Huitema in view of Harkins. The Applicants respectfully traverse the obviousness rejection of claims 4 and 22 because the combination of Huitema and Harkins fails to disclose or suggest all of the limitations of any of these claims.

First, claims 4 and 22 are dependent upon independent claims 1 and 17 respectively, which Applicants submit are in a condition for allowance. Since Huitema does not disclose all of the limitations of claims 1 and 17, Huitema necessarily does not disclose all of the limitations of claims 4 and 22.

Second, Harkins merely discloses a hybrid protocol for negotiating and providing authenticated keying material, for security associations in a protected manner. (Harkins, page 2, 5th para., lines 1-3). Although the Internet Key Exchange methods disclosed by

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

the combination of Huitema and Harkins involve the transmission of an Initiator cookie to a Responder and a Responder cookie to an Initiator, the combination does not disclose or suggest a method of distributed generation of unique random numbers for digital cookies.

In particular, the combination Huitema and Harkins does not disclose or suggest (i) generating a first portion of an x-bit digital cookie based on an x-bit mask template, or (ii) generating potential x-bit digital cookies until generating a potential x-bit digital cookie that is not in use on a computer network, or (iii) generating a complete x-bit digital cookie using the first and second portions of the x-bit digital cookie, as claimed in claim 1.

Also, in particular, the combination Huitema and Harkins does not disclose or suggest creating a complete digital cookie using an (x-n) bit random number, an x-bit random number, and an x-bit bit mask, or the sending, receiving, counting, or generating steps, as claimed in claim 17.

Because the combination of Huitema and Harkins fails to disclose or suggest all of the limitations of claims 4 and 22, a *prima facie* case of obviousness of these claims does not exist.

b. Claims 9, 16, 20, and 26

As noted above, claims 9, 16, 20, and 26 were rejected under 35 U.S.C. §103(a) as being unpatentable over Huitema in view of Montenegro. The Applicants respectfully traverse the obviousness rejection of claims 9, 16, 20, and 26 because the combination of Huitema and Montenegro fails to disclose or suggest all of the limitations of any of these claims.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

First, claims 9, 16, 20, and 26 are dependent upon independent claims 1, 10, 17, and 23 respectively. As noted above, Huitema does not disclose all of the limitations of claims 1, 10, 17, and 23. Thus, Huitema necessarily does not disclose all of the limitations of claims 9, 16, 20, and 26.

Second, Montenegro merely discloses an initiator cookie range parameter used in "realm specific internet protocol" (RSIP) extensions and mechanisms for "internet key exchange" (IKE) sessions, and (ii) new messages to transmit the cookie range.

Even if Huitema and Montenegro are combined, the combination still does not disclose or suggest all of the limitations of claims 9, 16, 20, and 26. Neither Huitema nor Montenegro disclose or suggest a method for generating a complete x-bit digital cookie not in use on a computer network.

In particular, the combination of Huitema and Montenegro does not disclose or suggest a method of generating a first portion of the x-bit digital cookie on a first network device, generating a second portion of the x-bit digital cookie on a second network device, and generating a complete x-bit digital cookie from the first and second portions, as claimed in claims 1 and 10. Furthermore, in particular, the combination of Huitema and Montenegro does not disclose or suggest using an (x-n) bit random number, an x-bit random number, and an x-bit bit mask to generate a complete digital cookie as claimed in claim 20 or using an n-bit random number and an (x-n) bit random number to create a complete x-bit digital cookie as claimed in claim 26. Since the combination of Huitema and Montenegro does not disclose or suggest all of the limitations of claims 1, 10, 17, and 26, the combination necessarily does not disclose or suggest all of the limitations of claims 9, 16, 20, and 26.

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001

Because the combination of Huitema and Montenegro fails to disclose or suggest all of the limitations of claims 9, 16, 20, and 26, a *prima facie* case of obviousness of these claims does not exist.

5. Conclusion

In view of the foregoing amendments and remarks, Applicants respectfully submit that all of the presently pending claims in the application are believed to be in condition for allowance. Applicants hereby earnestly solicit an early Notice of Allowance. The Examiner is invited to call the undersigned if the Examiner believes it would be helpful towards moving the case to issuance or resolving any further issues.

Respectfully submitted,

Dated: 8/9/04

By: _____

Robert J. Irvine III
Reg. No. 41,865
Attorney for Applicants
312-913-3305

McDONNELL BOEHNEN
HULBERT & BERGHOFF LLP
300 SOUTH WACKER DRIVE
CHICAGO, ILLINOIS 60606
TELEPHONE (312) 913-0001